PATENT ABSTRACTS OF JAPAN

(11)Publication number : 08-115277
(43)Date of publication of application : 07.05.1996

(51)Int.Cl. G06F 13/00
G06F 15/00

(21)Application number : 06-253339
(22)Date of filing : 19.10.1994

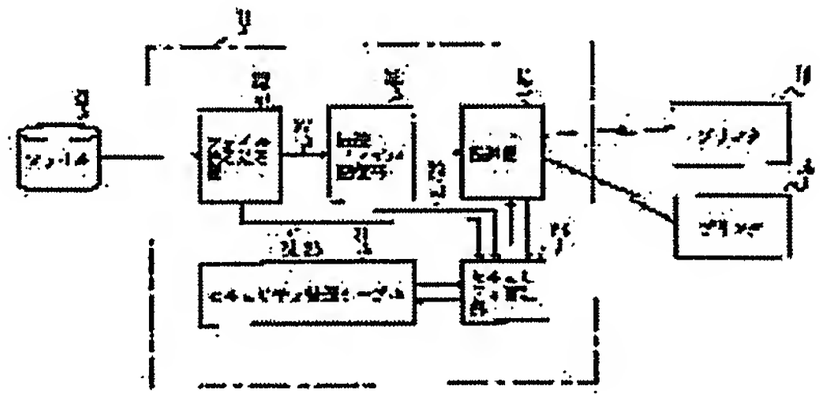
(71)Applicant : FUJI XEROX CO LTD
(72)Inventor : TANIHATA JUNJI

(54) FILE TRANSFER DEVICE

(57)Abstract:

PURPOSE: To realize the file transfer device in which the transfer of a file relatively high in security is taken into consideration.

CONSTITUTION: Security levels are written in files received by a file read part 22 in relation to transfer destinations. A security management part 26 registers respective transfer destinations and security levels of received files in a security management table 31; and at the time of transfer of a file, the security level of this file is compared with that of the transfer destination, and the file is transferred from a transfer part 41 only when the security level of the transfer destination is higher or security levels of both of them are equal to each other. Consequently, the file is not transferred to secure the safety if the destination designated as the transfer destination of the file has a lower security level.



CLAIMS

[Claim(s)]
[Claim 1]A file transfer device comprising:
The file side security information decoding means which decodes the file side security information about the confidentiality of the file been [a file / it] attached and described at a file.
An output-destination-information decoding means which decodes output destination information about an output destination change of the file been [a file / it] attached and described at a file.
An output destination change security information storing means which stored security information about those confidentiality beforehand for every output destination change of a file.
A security discriminating means which distinguishes whether security is secured or not when the file side security information and output destination change security information of an output destination change of a file which transmits are compared and a file is outputted to the output destination change, A file transfer means to transmit a file only to an output destination change presupposed that security is secured by a security discriminating means.

[Claim 2]A file transfer device comprising:
The file side security level information decoding means which decodes the file side security level information about the confidentiality of the file been [a file / it] attached and described at a file.
An output-destination-information decoding means which decodes output destination information about an output destination change of the file been [a file / it] attached and described at a file.
An output destination change security level information storing means which stored security level information about those confidentiality beforehand for every output destination change of a file.
A security discriminating means to which the file side security level information and an output destination change security information level of an output destination change of a file which transmits are compared, both level is equal, or transmission of a file is permitted to the output destination change only when a direction of an output destination change has an expensive level of security, A file transfer means to transmit a file only to an output destination change where transmission was permitted by a security discriminating means.

[Claim 3]A file transfer device comprising:
The file side security level information decoding means which decodes the file side security level information about the confidentiality of the file been [a file / it] attached and described at a file.
An output-destination-information decoding means which decodes output destination information about an output destination change of the file been [a file / it] attached and described at a file.
An output destination change security level information storing means which stored security level information about those confidentiality beforehand for every output destination change of a file.
A security discriminating means to which the file side security level information and an output destination change security information level of an output destination change of a file which transmits are compared, and transmission of a file is permitted to the output destination change only when both level is equal, A file transfer means to transmit a file only to an output destination change where transmission was permitted by a security discriminating means.

[Claim 4]A file transfer device comprising:

The file side security information decoding means which decodes the file side security information about the confidentiality of the file been [a file / it] attached and described at a file.
An output-destination-information decoding means which decodes output destination information about an output destination change of the file been [a file / it] attached and described at a file.
An output destination change security information storing means which stored beforehand output destination change security information about those confidentiality for every output destination change of a file.
A security management table preparing means which creates a security management table which transmits, and which matched and stored those output destination changes and the file side security information for every file, Whenever a transfer request of a file arises, by a security management table preparing means. A file multiple address transfer means which performs multiple address transmission only to an output destination change presupposed that output destination change security information stored in a created security management table and an output destination change security information storing means is compared, and security is secured for every file.

[Translation done.]

DETAILED DESCRIPTION

[Detailed Description of the Invention]
[0001]
[Industrial Application]This invention relates to the file transfer device which transmits a file using the means of communication of a Local Area Network etc., The file which needs to have secrecy held in detail is also related with the file transfer device which enabled it to secure confidentiality in the case of outputs, such as the print-out, or use of a file.
[0002]
[Description of the Prior Art]What is necessary is just to print out in this, if the printer is directly linked with the information processor which stored the file when trying to print the created various files. Therefore, whether the confidentiality of the file is high does not pose a problem in particular in the situation where printing out a file or displaying on CRT is maintaining identity by the relation with the maker of a file.
[0003]However, if many computers, a workstation, or an information processor like a word processor comes to be arranged in an office, The concept which shares the setting position of a printer and the preservation part of a file will arise, and Local Area Networks, such as Ethernet, will spread. In such a communications system, the printer is arranged here and there [of the telecommunication cable]. Corresponding to the printer of the place near oneself, or the character of documents to print out, when printing [everybody] in a color, even if somewhat far, they choose the printer which fills the demand, transmit a file, and they make it print.
[0004]Thus, if it comes to share a printer or output equipment, how the high file of confidentiality should be processed will pose a problem. The proposal which discharged the printed documents as a way method for the solution on the tray which a key requires is performed. When such a technique was not able to be taken, printing with the printer with which confidentiality is secured rather than transmitting the file to a printer electronically, putting this into an envelope, and delivering to the other party as mail in the company or usual mail was performed.
[0005]
[Problem(s) to be Solved by the Invention]However, since the printer which has arranged the special tray which a key requires needed to be addressed, it needed to specify first and the file needed to be transmitted when the former technique was adopted, such a special printer was needed. When there were few such printers, the tray which a key requires decreased as compared with the number of those who receive printed matter, and there was a problem that the case where the tray cannot necessarily be used arose. There was a problem also in respect of storage of a key or management.
[0006]In the case of the technique by latter mail or mail, since the transmitting side needed to perform printing and dispatch of a file, when you needed documents immediately, there is not only a problem of taking time and effort, but there was a problem that this could not be coped with.
[0007]As mentioned above, although the problem about transmission of the high file of the confidentiality in the former was explained, when carrying out the simultaneous transmissive communication of the one file to two or more places connected to the telecommunication cable from one device, or in transmitting without a sending person doing the direct control of the file, it also generates a new problem. That is, when a file is transmitted indirectly in this way, it is because the file will be automatically transmitted by distinction of whether the file is what requires

secrecy not being performed by the sending person, but performing predetermined transfer procedures. For example, although decreasing the number of times of reading of the data transmitted in order to raise the transmission processing performance in simultaneous transmissive communication is proposed by JP,4-192052,A, there is no consideration which was mentioned above in it.
[0008]Then, the 1st purpose of this invention is to provide the file transfer device which can transmit the file in consideration of confidentiality.
[0009]The 2nd purpose of this invention is to provide the file transfer device which can transmit a file in consideration of the level and character of confidentiality.
[0010]There is the 3rd purpose of this invention in providing the file transfer device which can hold confidentiality, when performing simultaneous transmissive communication.
[0011]
[Means for Solving the Problem]The file side security information decoding means which decodes the file side security information about the confidentiality of the file been [a file / it] attached and described by the invention according to claim 1 at a (b) file, (**) An output-destination-information decoding means which decodes output destination information about an output destination change of the file been [a file / it] attached and described at a file, (**) An output destination change security information storing means which stored security information about those confidentiality beforehand for every output destination change of a file, (**) A security discriminating means which distinguishes whether security is secured or not when the file side security information and output destination change security information of an output destination change of a file which transmits are compared and a file is outputted to the output destination change, (**) Make a file transfer device possess a file transfer means to transmit a file only to an output destination change presupposed that security is secured by a security discriminating means.
[0012]Namely, in the invention according to claim 1, acquire this information from a file which described the file side security information, and. Those output destination change security information was acquired for every output destination change of a file, and these were compared on the occasion of transmission of a file, it decided to transmit a file only to an output destination change presupposed that security is secured, and confidentiality is secured.
[0013]The file side security level information decoding means which decodes the file side security level information about the confidentiality of the file been [a file / it] attached and described by the invention according to claim 2 at a (b) file, (**) An output-destination-information decoding means which decodes output destination information about an output destination change of the file been [a file / it] attached and described at a file, (**) An output destination change security level information storing means which stored security level information about those confidentiality beforehand for every output destination change of a file, (**) A security discriminating means to which the file side security level information and an output destination change security information level of an output destination change of a file which transmits are compared, both level is equal, or transmission of a file is permitted to the output destination change only when a direction of an output destination change has an expensive level of security, (**) Make a file transfer device possess a file transfer means to transmit a file only to an output destination change where transmission was permitted by a security discriminating means.
[0014]Namely, acquire security level information on the file been [a file / it] attached and described by the invention according to claim 2 at a file, and. Those output destination change security level information is acquired for every output destination change of a file, A security level of a file is equal to the destination, or when the destination is higher, he is trying to compare these levels for every destination in the case of transmission of a file, and to permit transmission as what security is secured.
[0015]The file side security level information decoding means which decodes the file side security level information about the confidentiality of the file been [a file / it] attached and described by the invention according to claim 3 at a (b) file, (**) An output-destination-information decoding means which decodes output destination information about an output destination change of the file been [a file / it] attached and described at a file, (**) An output destination change security level

information storing means which stored security level information about those confidentiality beforehand for every output destination change of a file, (**) A security discriminating means to which the file side security level information and an output destination change security information level of an output destination change of a file which transmits are compared, and transmission of a file is permitted to the output destination change only when both level is equal, (**) Make a file transfer device possess a file transfer means to transmit a file only to an output destination change where transmission was permitted by a security discriminating means.
[0016]Namely, acquire security level information on the file been [a file / it] attached and described by the invention according to claim 3 at a file, and. Those output destination change security level information is acquired for every output destination change of a file, and these levels are compared for every destination in the case of transmission of a file, and only when a security level of a file is equal to the destination, he is trying to permit transmission as what security is secured. That is, also when a level of security does not necessarily have the hierarchical order, it decided to transmit a file only to the equal destination of a level, and reservation of security is realized.
[0017]The file side security information decoding means which decodes the file side security information about the confidentiality of the file been [a file / it] attached and described by the invention according to claim 4 at a (b) file, (**) An output-destination-information decoding means which decodes output destination information about an output destination change of the file been [a file / it] attached and described at a file, (**) An output destination change security information storing means which stored beforehand output destination change security information about those confidentiality for every output destination change of a file, (**) A security management table preparing means which creates a security management table which transmits, and which matched and stored those output destination changes and the file side security information for every file, (**) Whenever a transfer request of a file arises, by a security management table preparing means. A file transfer device is made to possess a file multiple address transfer means which performs multiple address transmission only to an output destination change presupposed that output destination change security information stored in a created security management table and an output destination change security information storing means is compared, and security is secured for every file.
[0018]Namely, it is for the invention according to claim 4 securing security at the time of performing multiple address transmission to two or more destinations, Information on the destination that acquire this information from a file which described the file side security information, and simultaneous transmissive communication is performed is acquired, A security management table showing a relation with security information of each destination for simultaneous transmissive communication is created, Reservation of confidentiality is realized as each destination and security information of a file were compared based on this table when performing simultaneous transmissive communication, and multiple address transmission was performed to an output destination change presupposed that security is secured. Multiple address transmission may be a thing of a type transmitted one by one, or it may bundle up to the destination and it may be transmitted to it.
[0019]
[Example]This invention is explained in detail per example below.
[0020]Drawing 1 expresses the outline of the communications system which uses the file transfer device in one example of this invention. The file transfer device 11 of this example is connected to the telecommunication cable 12. this telecommunication cable 12 -- the [the 1st -] -- the 1st - the Mth printer $14_{\text{the 1}}$ - 14_M are also connected besides workstation (WS)13_1 of N - 13_N. The 1st - the Nth workstation $13_{\text{the 1}}$ - 13_N transmit the file to the file transfer device 11, when you wish print-out of the created file. The file transfer device 11 makes it print by transmitting this to what it was specified of the 1st - the Mth printer $14_{\text{the 1}}$ - the 14_M as. It is also possible to transmit a file to the printer of other communications systems via the communications server which the file transfer device 11 does not need to transmit a file within the limits of the communication network shown in this figure, for example, is not illustrated.

[0021]Drawing 2 expresses the composition of a file transfer device theoretically. If the file 21 is sent from either the 1st which showed drawing 1 the file transfer device 11 – the Nth workstation $13_{\text{the 1}}$ – 13_N, the file reading part 22 will receive this. The file reading part 22 reads a file attribute record and a security–attributes record from each file. And the basic information 23, such as a file name, is acquired from a file attribute record, and the security information 24 comes to hand from a security–attributes record. In this stage, these basic information 23 and the security information 24 are sent out to the security management department 26, and are memorized as a reference value, respectively.
[0022]If the file reading part 22 is taken out from the file which received the live data 27 following a security–attributes record, it will transmit this to the transfer file storage parts store 28. If the live data 27 are received, the transfer file storage parts store 28 stores this in the memory arranged inside one by one, and when storing is completed, it will notify the storing completion notification 29 to the security management department 26.
[0023]The security management department 26 will discover the table entry of the file which transmits with reference to the contents of the security management table 31, if the storing completion notification 29 is received. And destination information is taken out sequentially from an applicable table entry. And these are sent to the transfer part 41 in order, and it transmits to the printer 14 directed on the security management table 31. At this time, the security management department 26 will permit transmission to the printer 14 without a security top problem. The details of the transfer control of a file are explained later.
[0024]Although the file transfer device 11 whole of such composition does not illustrate, it is provided with CPU (central processing unit), Various control of the transfer control of a file, etc. is performed using the operating memory etc. which store temporarily ROM (read only memory), various data, and the file or table that stored various control programs.
[0025]Drawing 3 expresses the composition of a security management table. In the security management table 31, the addresses A and those security levels L of the name of the file to transmit and the destination of these files are describing. According to such environment placed, one stage of five steps of inside is defined about the 1st which showed drawing 1 the security level L – Mth printer 14_1–14_M. These stages and a person's correspondence which can be known are as follows, for example.
[0026]
[Table 1]

セキュリティレベル	内容
"L_0"	機密上の問題なし
"L_1"	グループリーダ相当以上
"L_2"	課長相当以上
"L_3"	部長相当以上
"L_4"	最高機密

[0027]The state of each security level of the 1st – the Mth printer $14_{\text{the 1}}$ – 14_M is set to the security level table which is not illustrated, The workstation used as the master of the 1st – the Nth workstation $13_{\text{the 1}}$ – the 13_N can set up these levels, and they can change the contents. Drawing 3 shows that the security level of 1st printer 14_1 as the 1st destination is set as "L_2", and that the security level of Nth printer 14_N is set as "L_0." For example, since it is not premised on persons other than post as a section chief using it on the assumption that it is used, in order that plurality or a single section chief may receive 1st printer 14_1 the documents of personnel relations, etc. in the same part, the security level is high a little. On the other hand, since Nth printer 14_N is arranged at the place which the usual researcher etc. can use freely, the security level serves as the minimum.
[0028]Of course, the classification of a security level is possible in some numbers except having been shown in Table 1, for example, it is also possible to use a confidential to the outside of the

company level and "L_3" as a secret level, and to use ["L_0" / a common level and "L_1"] "L_4" as a strictly confidential level for a handling caution level and "L_2." The number of levels is not restricted to this, either.

[0029]Drawing 4 expresses the composition of the file which a file transfer device receives. The file 32 sent to the file transfer device 11 has the composition that the file attribute record 34 and the security-attributes record 35 were added to the live data 33 which make the contents of a file. On the file attribute record 34, the information of a file name, the owner of a file, the transmission destination which wishs, etc., etc. is describing.

On the security-attributes record 35, either [of the file / five steps of] security level L_0 - L_4 are describing.

However, in the system of this example, when there is no statement of the security level L, the legal fiction of this is carried out to security level L_0. That is, the file transfer device of this example is aiming at those practical use because the existing file which does not have the file organization shown in drawing 4 also carries out the ** system of the security level to L_0.

[0030]Drawing 5 expresses concretely the situation of the transfer control of the file by a file transfer device. If there is a storing completion notification to a series of files as described above (step S101;Y), the value of the two variables a and b will be initialized by "1", respectively (Step S102). These variables a and b are stored in the predetermined field of the above mentioned operating memory. The above mentioned CPU reads security level L_f about file F_1 of the 1st table entry of the security management table 31 shown in drawing 3 (Step S103). This is stored in the security-attributes record 35 of the file 32 shown in drawing 4. And security level L_P of the 1st destination (the 1st printer 14_1) is read (Step S104). Here, security level L_P is "L_0." And since security level L_f is equal to security level L_P, or the problem of (Step S105; N) and security does not occur in being lower than this, the file F_1 is transmitted to the applicable destination (Step S106).

[0031]In the case of this example, suppose that security level L_f about file F_1 of the 1st table entry is "L_1." Then, since "L_1" is smaller than "L_2" as security level L_P of the destination, the problem of security does not occur. Therefore, file F_1 will be transmitted to the 1st destination (the 1st printer 14_1) from the transfer part 41. Of course at this time, address A_1 of that destination registered into the security management table 31 is notified to the transfer part 41.

[0032]Then, the value of the variable b counts up only "1" and is set to "2" (Step S107). It is investigated on the security management table 31 whether CPU has the 2nd destination about file F_1 (Step S108). And as long as the destination exists, it returns to Step S104 and the same check is performed, and when fulfilling the conditions of Step S105, transmission of file F_1 will be performed to the destination.

[0033]The control content over the directions which transmit file F_1 to Nth printer 14_N as other examples is explained. In this case, security level L_P of the n-th destination (the Nth printer 14_N) is "L_0" to security level L_f about file F_1 being "L_1." In judgment of Step S105, the direction of security level L_f about file F_1 becomes large, and the destination will have a security top problem (N). Therefore, transmission of file F_1 to Nth printer 14_N by the transfer part 41 will not be permitted in this case, but it will progress to Step S107 promptly, and processing about the next destination will be performed.

[0034]Since the n-th destination (the Nth printer 14_N) becomes about file F_1 in the last destination in the case of this example (step S108;N), shortly, the variable a counts up only "1" and is set to "2" (Step S109). Since the data about the file which should be transmitted to the next is set to the security management table 31 (step S110;Y), It will progress to Step S103 and same transfer control about file F_2 of the 2nd entry table will be performed (Steps S103-S110).

Thus, after transmission processing is completed about all the files set to the security management table 31 (step S110;N), the control about a series of file transfers is completed (end).
[0035]In the example described above, when distinguishing a security level at Step S105 of drawing 5, and it was more than the level with which the level of the destination of a file is demanded when transmitting a file, it decided to transmit the file. This leaves for the premise of not producing a security top problem even if it outputs the file distributed among a certain section chief, for example to the printer which the manager owns. However, it may be appropriate for a security level to be necessarily unable to define by the hierarchical order of a level depending on the contents of the system to build, but to be outputted only to the printer or the destination of the same security level. In such a system, the file transfer device of this invention may perform control which is transmitted only to the destination of the same security level (the invention according to claim 3).
[0036]Although the example explained the case where the destination of a file was a printer, It is also possible to make into the destination document preparation devices, such as not the thing to restrict to this but a display device and a word processor into which the file which received depending on the case is edited, and this invention can be applied also to these. For example, in the system shown in drawing 1, if there is a security top problem also when the simultaneous transmissive communication of the file which 1st workstation 13_1 created, for example is carried out to the 4th – the 8th workstation $13_{\text{the 4}}$ – 13_8, this invention is effectively utilizable.
[0037]In the example, even if the destination of a file was proper on security, the case where transmission went wrong with busy one etc. was not explained. In such a case, if it leaves the destination in which transmission failed, and an applicable file name to the security management table 31, these files can be transmitted to the untransmitted destination at the time of occasions when the following storing completion notification (Step S101) occurs. If a file is transmitted to all the destinations which are not made into a security top problem, of course, the applicable entry in the security management table 31 may also be deleted. Naturally to the destination to which a file was not transmitted noting that there was a security top problem, a notice to that effect may be performed separately.
[0038]Although the example explained multiple address transmission of the serial simultaneous transmissive communication type which transmits the sequential file to the destination, Naturally this invention is applicable to multiple address transmission of the package simultaneous transmissive communication type which checks security about each destination and transmit the file all at once about what passed. In order to perform such package simultaneous transmissive communication in a Local Area Network, For example, the address common to the device of reception destinations, such as each printer, is attached, a file is transmitted, or these addresses are written together, a file is transmitted, and the device which these–corresponds should just incorporate the file in common.
[0039]
[Effect of the Invention]As explained above, according to the invention according to claim 1, acquire this information from the file which described the file side security information, and. Since it decided to transmit a file only to the output destination change presupposed that those output destination change security information is acquired for every output destination change of a file, these are compared in the case of transmission of a file, and security is secured, Maintenance of confidentiality is securable even if the sending person of a file does not have the knowledge about the security of the destination.
[0040]According to the invention according to claim 2, acquire the security level information on the file been [a file / it] attached and described at the file, and. Those output destination change security level information is acquired for every output destination change of a file, On the occasion of transmission of a file, these levels were compared for every destination, the security level of a file was equal to the destination, or when the destination was higher, transmission was permitted as what security is secured. Thus, since the level was set up about the strength of security, even if the sending person of a file does not have the knowledge about the security of the destination, Transmission will be performed only to the destination which can secure the security more than the set–up level, and maintenance of confidentiality can be secured.
[0041]According to the invention according to claim 3, acquire the security level information on the

file been [a file / it] attached and described at the file, and. Those output destination change security level information was acquired for every output destination change of a file, these levels were compared for every destination on the occasion of transmission of a file, and only when the security level of a file was equal to the destination, transmission was permitted as what security is secured. Thus, since it decided to transmit only to the destination in which the sending person of a file forms a level in the security of the destination, and the set-up level corresponds since the level was set up about the strength of security, Maintenance of confidentiality can be secured even when the level of security does not necessarily have the hierarchical order.
[0042]The information on the destination that acquire this information from the file which described the file side security information according to the invention according to claim 4, and simultaneous transmissive communication is performed is acquired, The security management table showing a relation with the security information of each destination for simultaneous transmissive communication is created, When performing simultaneous transmissive communication, each destination and the security information of a file are compared based on this table, and it was made to perform multiple address transmission to the output destination change presupposed that security is secured. Therefore, simultaneous transmissive communication can be smoothly performed using a security management table. If the existence of a success of transmission is recorded on a table, it can transmit at the next time, securing security also about the untransmitted destination.
[0043]Since a file is transmitted to two or more destinations in the case of simultaneous transmissive communication, Since data concerning [a stake] this by the invention according to claim 4 for acquiring the information about the security of these destinations is prepared for the file transfer device side and a security management table is created based on this, The sending person should just specify the destination expected that security information is described at a file, and is effective in simultaneous transmissive communication work increasing the efficiency.

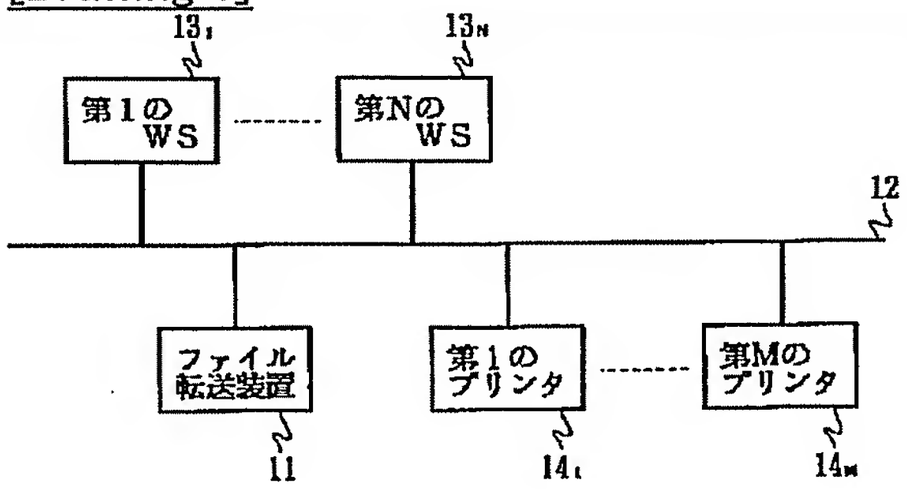
[Translation done.]

DESCRIPTION OF DRAWINGS

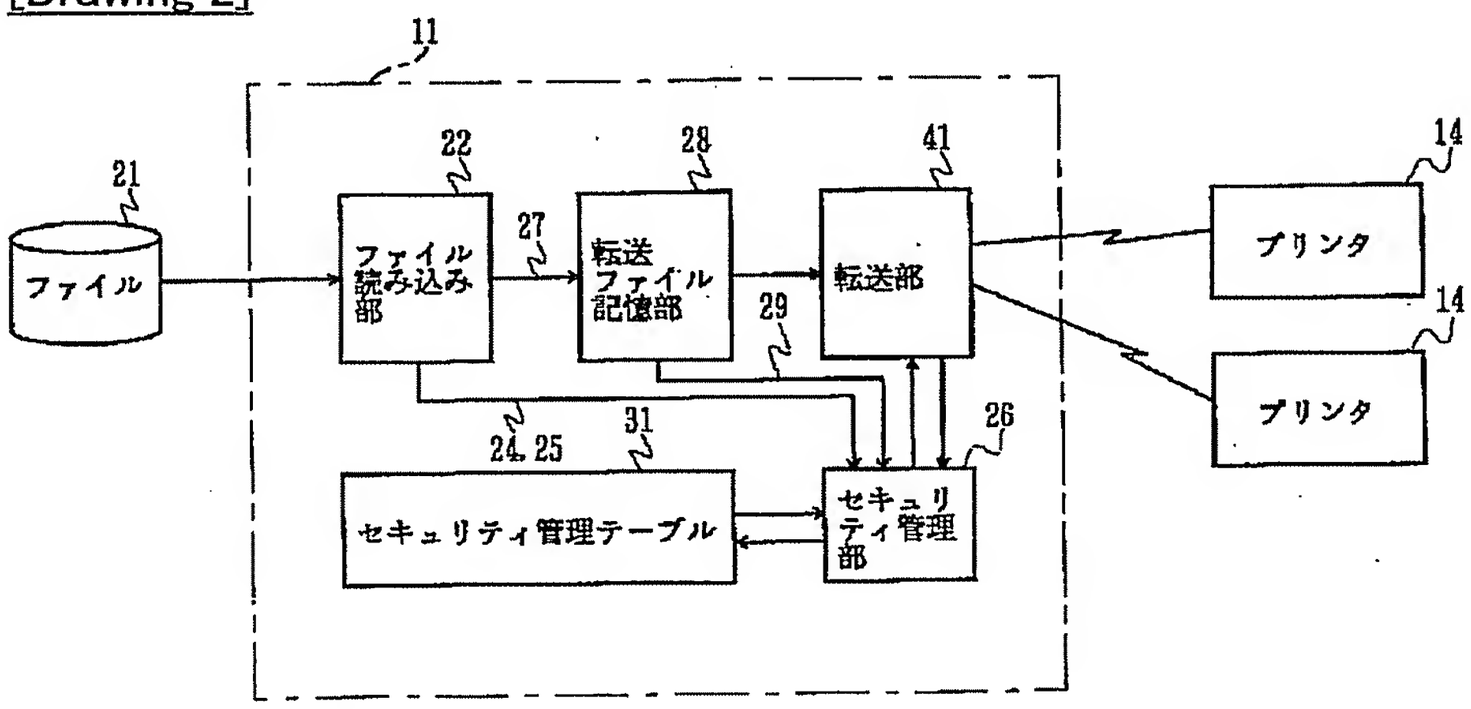
[Brief Description of the Drawings]
[Drawing 1]It is a system configuration figure showing the outline of the communications system which uses the file transfer device in one example of this invention.
[Drawing 2]It is the block diagram which expressed the composition of the file transfer device of this example theoretically.
[Drawing 3]It is an explanatory view showing the composition of the security management table in this example.
[Drawing 4]It is an explanatory view showing the composition of the file which the file transfer device of this example receives.
[Drawing 5]It is the flow chart which expressed concretely the situation of the transfer control of the file by a file transfer device.
[Description of Notations]
11 -- A file transfer device, 14_1-14_M -- The 1 - the Mth printer, 21, 32 [-- A transfer file storage parts store, 31 / -- A security management table, 35 / -- A security-attributes record, L / -- Security level] -- A file, 22 -- A file reading part, 26 -- A security management department, 28

DRAWINGS

[Drawing 1]



[Drawing 2]

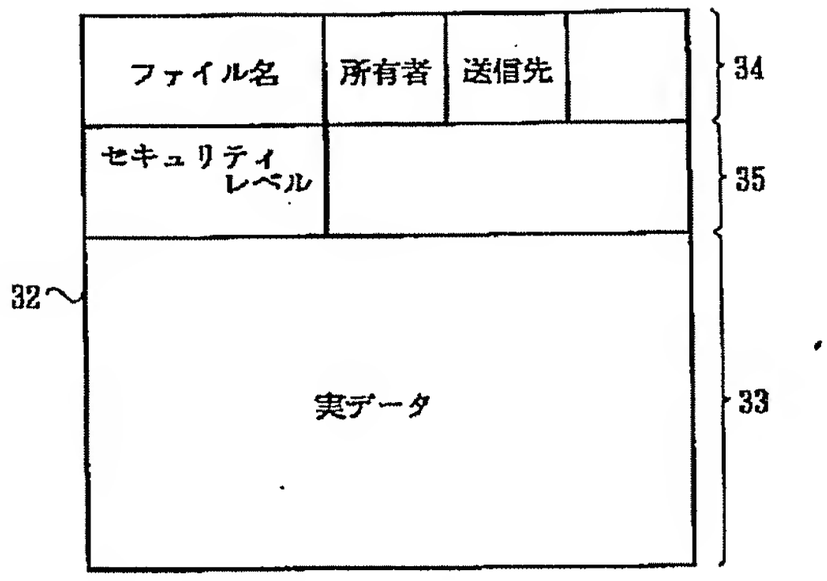


[Drawing 3]

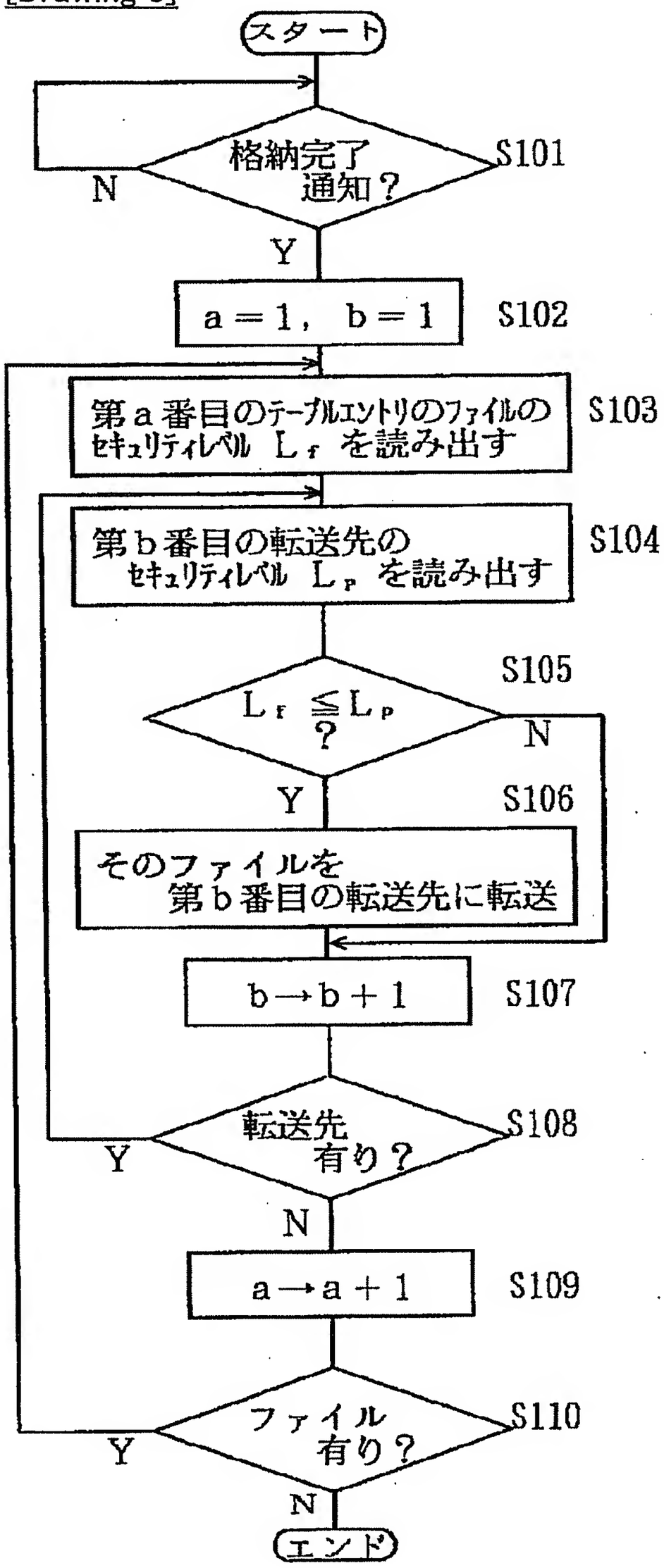
31

ファイル名	第1の転送先		……	第nの転送先	
	アドレス	セキュリティレベル		アドレス	セキュリティレベル
F₁	A₁	L₂	……	AN	L₀
F₂	AN	L₀			
⋮					

[Drawing 4]


ファイル名
所有者
送信先
セキュリティ
レベル
実データ
32
34
35
33

[Drawing 5]


スタート
格納完了
通知？
S101
N
Y
a＝1， b＝1
S102
第ａ番目のテーブルエントリのファイルの
セキュリティレベル Ｌｆ を読み出す
S103
第ｂ番目の転送先の
セキュリティレベル Ｌｐ を読み出す
S104
Ｌｆ ≦ Ｌｐ
？
S105
N
Y
S106
そのファイルを
第ｂ番目の転送先に転送
b→b＋1
S107
転送先
有り？
S108
Y
N
a→a＋1
S109
ファイル
有り？
S110
Y
N
エンド

引用例3

(19)日本国特許庁（ＪＰ）　(12)**公開特許公報**（Ａ）　(11)特許出願公開番号

特開平8－115277

(43)公開日　平成８年(1996)５月７日

(51)Int.Cl.[6]		識別記号	庁内整理番号	ＦＩ	技術表示箇所
Ｇ０６Ｆ	13/00	３５１　Ｅ	7368－5E		
	15/00	３３０　Ｄ	9364－5L		

審査請求　未請求　請求項の数４　ＯＬ　（全９頁）

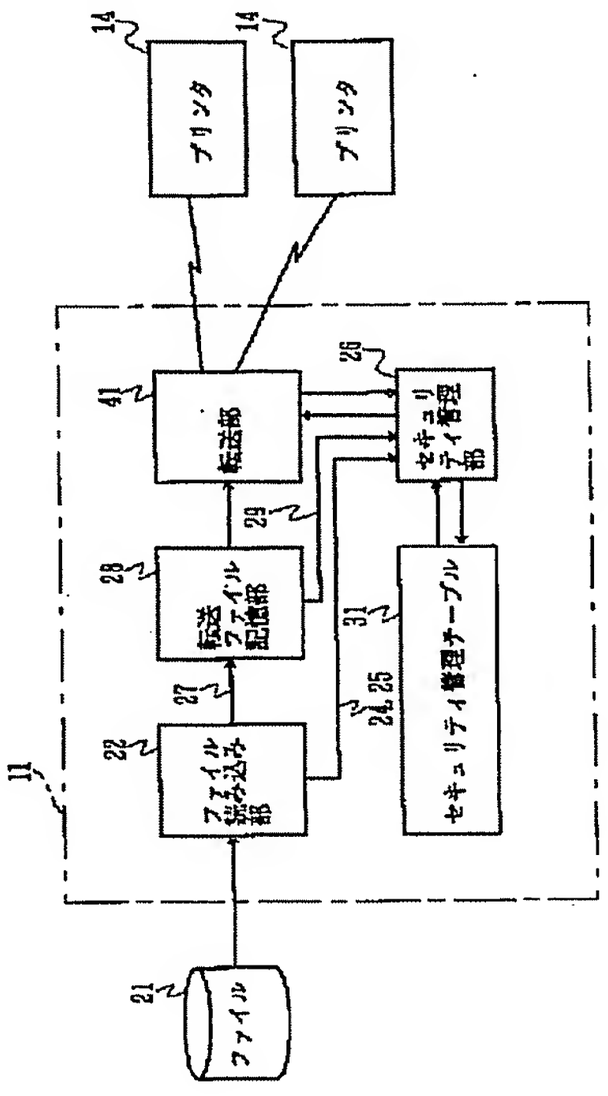
(21)出願番号　特願平6－253339

(22)出願日　平成６年(1994)10月19日

(71)出願人　000005496
富士ゼロックス株式会社
東京都港区赤坂三丁目３番５号
(72)発明者　谷畑　淳司
埼玉県岩槻市府内３丁目７番１号　富士ゼロックス株式会社岩槻事業所内
(74)代理人　弁理士　山内　梅雄

(54)【発明の名称】　ファイル転送装置

(57)【要約】
【目的】　機密性が比較的高いファイルの転送に考慮したファイル転送装置を実現する。
【構成】　ファイル読み込み部２２が受信するファイルには転送先との関係でセキュリティレベルが記されている。セキュリティ管理部２６は、セキュリティ管理テーブル３１に受信したファイルのそれぞれの転送先とそれらのセキュリティレベルを登録しておき、ファイルの転送に際してファイル側のセキュリティレベルと比較して転送先の方が高いか両者が等しいレベルのときのみ転送部４１からそのファイルの転送を行わせる。したがって、ファイルの転送先として指定された宛て先がセキュリティレベルが低い場合にはこれに対する転送が行われず、安全性が確保される。



1

【特許請求の範囲】
【請求項１】　ファイルに付属して記されたそのファイルの機密性に関するファイル側セキュリティ情報を解読するファイル側セキュリティ情報解読手段と、
ファイルに付属して記されたそのファイルの出力先に関する出力先情報を解読する出力先情報解読手段と、
ファイルの出力先ごとにそれらの機密性に関するセキュリティ情報を予め格納した出力先セキュリティ情報格納手段と、
送信するファイルのファイル側セキュリティ情報とその出力先の出力先セキュリティ情報とを照合しその出力先にファイルを出力したときセキュリティが確保されるかどうかを判別するセキュリティ判別手段と、
セキュリティ判別手段によってセキュリティが確保されるとされた出力先にのみファイルを転送するファイル転送手段とを具備することを特徴とするファイル転送装置。
【請求項２】　ファイルに付属して記されたそのファイルの機密性に関するファイル側セキュリティレベル情報を解読するファイル側セキュリティレベル情報解読手段と、
ファイルに付属して記されたそのファイルの出力先に関する出力先情報を解読する出力先情報解読手段と、
ファイルの出力先ごとにそれらの機密性に関するセキュリティレベル情報を予め格納した出力先セキュリティレベル情報格納手段と、
送信するファイルのファイル側セキュリティレベル情報とその出力先の出力先セキュリティ情報レベルとを照合し両者のレベルが等しいか出力先の方がセキュリティのレベルが高いときのみその出力先にファイルの転送を許可するセキュリティ判別手段と、
セキュリティ判別手段によって転送が許可された出力先にのみファイルを転送するファイル転送手段とを具備することを特徴とするファイル転送装置。
【請求項３】　ファイルに付属して記されたそのファイルの機密性に関するファイル側セキュリティレベル情報を解読するファイル側セキュリティレベル情報解読手段と、
ファイルに付属して記されたそのファイルの出力先に関する出力先情報を解読する出力先情報解読手段と、
ファイルの出力先ごとにそれらの機密性に関するセキュリティレベル情報を予め格納した出力先セキュリティレベル情報格納手段と、
送信するファイルのファイル側セキュリティレベル情報とその出力先の出力先セキュリティ情報レベルとを照合し両者のレベルが等しいときのみその出力先にファイルの転送を許可するセキュリティ判別手段と、
セキュリティ判別手段によって転送が許可された出力先にのみファイルを転送するファイル転送手段とを具備することを特徴とするファイル転送装置。

2

【請求項４】　ファイルに付属して記されたそのファイルの機密性に関するファイル側セキュリティ情報を解読するファイル側セキュリティ情報解読手段と、
ファイルに付属して記されたそのファイルの出力先に関する出力先情報を解読する出力先情報解読手段と、
ファイルの出力先ごとにそれらの機密性に関する出力先セキュリティ情報を予め格納した出力先セキュリティ情報格納手段と、
送信するファイルごとにそれらの出力先とファイル側セキュリティ情報とを対応付けて格納したセキュリティ管理テーブルを作成するセキュリティ管理テーブル作成手段と、
ファイルの転送要求が生じるたびにセキュリティ管理テーブル作成手段によって作成されたセキュリティ管理テーブルと出力先セキュリティ情報格納手段に格納された出力先セキュリティ情報を照合してファイルごとにセキュリティが確保されるとされた出力先にのみ同報転送を行うファイル同報転送手段とを具備することを特徴とするファイル転送装置。
【発明の詳細な説明】
【０００１】
【産業上の利用分野】本発明は例えばローカルエリアネットワーク等の通信手段を用いてファイルの転送を行うファイル転送装置に係わり、詳細には機密を保持される必要があるファイルでもそのプリントアウト等の出力あるいはファイルの利用の際に機密性を確保できるようにしたファイル転送装置に関する。
【０００２】
【従来の技術】作成した各種ファイルの印刷を行おうとする場合、そのファイルを格納した情報処理装置にプリンタを直結していれば、これにプリントアウトすればよい。したがって、そのファイルが機密性の高いものであるかどうかということは、ファイルをプリントアウトしたりＣＲＴに表示することがファイルの作成者との関係で同一性を保っている状況では特に問題となることはない。
【０００３】ところが、オフィスに多くのコンピュータやワークステーションあるいはワードプロセッサのような情報処理装置が配置されるようになると、プリンタの設置場所やファイルの保存箇所を共有する概念が生じ、イーサネット等のローカルエリアネットワークが普及することになった。このような通信システムでは、通信ケーブルの随所にプリンタが配置されている。各人は自分に近い場所のプリンタやプリントアウトする書類の性格に応じて、例えばカラーで印字を行う場合等には多少遠くてもその要求を満たすプリンタを選択してファイルを転送し、プリントを行わせるようになっている。
【０００４】このようにプリンタあるいは出力機器を共有するようになると、機密性の高いファイルをどのように処理すべきかが問題となる。その解決のための一手法

として、プリントした書類を鍵のかかるトレイに排出するようにした提案が行われている。このような手法をとることができない場合には、そのファイルを電子的にプリンタに転送するのではなく、機密性の確保されるプリンタでプリントし、これを封筒に入れて社内のメールまたは通常の郵便物として相手側に配送することが行われていた。

【０００５】

【発明が解決しようとする課題】しかしながら、前者の手法を採用すると鍵のかかる特別のトレイを配置したプリンタを宛て先に指定してファイルの転送を行う必要があるので、そのような特別のプリンタを必要とした。また、そのようなプリンタの数が少ないような場合には、鍵のかかるトレイが印刷物を受け取る者の数に比較して少なくなり、そのトレイを必ずしも利用することができない場合が生じるといった問題があった。また、鍵の保管や管理の点でも問題があった。

【０００６】また後者のメールまたは郵便物による手法の場合には、送信側がファイルの印刷や発送を行う必要があるので、手間がかかるといった問題があるだけでなく、書類を緊急に必要とする場合にはこれに対処することができないといった問題があった。

【０００７】以上、従来での機密性の高いファイルの転送についての問題点を説明したが、１か所の装置から通信ケーブルに接続された複数箇所に１つのファイルを同報通信する場合や、ファイルを送信者が直接操作することなく転送する場合には、新たな問題も発生する。すなわち、このようにファイルが間接的に転送される際には、そのファイルが機密を要するものであるかどうかの判別が送信者によって行われず、所定の転送手順を実行することでそのファイルが自動的に送信されることになるからである。例えば特開平４－１９２０５２号公報には、同報通信における転送処理性能を向上させるために転送するデータの読み込みの回数を減少させることが提案されているが、上述したような配慮はない。

【０００８】そこで本発明の第１の目的は、機密性を考慮したファイルの転送を行うことのできるファイル転送装置を提供することにある。

【０００９】本発明の第２の目的は、機密性のレベルや性格を考慮してファイルの転送を行うことのできるファイル転送装置を提供することにある。

【００１０】本発明の第３の目的は、同報通信を行う場合に機密性を保持することのできるファイル転送装置を提供することにある。

【００１１】

【課題を解決するための手段】請求項１記載の発明では、（イ）ファイルに付属して記されたそのファイルの機密性に関するファイル側セキュリティ情報を解読するファイル側セキュリティ情報解読手段と、（ロ）ファイルに付属して記されたそのファイルの出力先に関する出力先情報を解読する出力先情報解読手段と、（ハ）ファイルの出力先ごとにそれらの機密性に関するセキュリティ情報を予め格納した出力先セキュリティ情報格納手段と、（ニ）送信するファイルのファイル側セキュリティ情報とその出力先の出力先セキュリティ情報とを照合しその出力先にファイルを出力したときセキュリティが確保されるかどうかを判別するセキュリティ判別手段と、（ホ）セキュリティ判別手段によってセキュリティが確保されるとされた出力先にのみファイルを転送するファイル転送手段とをファイル転送装置に具備させる。

【００１２】すなわち請求項１記載の発明では、ファイル側セキュリティ情報を記しておいたファイルからこの情報を得ると共に、ファイルの出力先ごとにそれらの出力先セキュリティ情報を得て、ファイルの転送の際にはこれらを比較しセキュリティが確保されるとされた出力先にのみファイルを転送することにして、機密性を確保している。

【００１３】請求項２記載の発明では、（イ）ファイルに付属して記されたそのファイルの機密性に関するファイル側セキュリティレベル情報を解読するファイル側セキュリティレベル情報解読手段と、（ロ）ファイルに付属して記されたそのファイルの出力先に関する出力先情報を解読する出力先情報解読手段と、（ハ）ファイルの出力先ごとにそれらの機密性に関するセキュリティレベル情報を予め格納した出力先セキュリティレベル情報格納手段と、（ニ）送信するファイルのファイル側セキュリティレベル情報とその出力先の出力先セキュリティ情報レベルとを照合し両者のレベルが等しいか出力先の方がセキュリティのレベルが高いときのみその出力先にファイルの転送を許可するセキュリティ判別手段と、（ホ）セキュリティ判別手段によって転送が許可された出力先にのみファイルを転送するファイル転送手段とをファイル転送装置に具備させる。

【００１４】すなわち請求項２記載の発明では、ファイルに付属して記されたそのファイルのセキュリティレベル情報を得ると共に、ファイルの出力先ごとにそれらの出力先セキュリティレベル情報を得て、ファイルの転送の際には転送先ごとにこれらのレベルを比較し、ファイルのセキュリティレベルが転送先と等しいか転送先の方が高い場合にはセキュリティが確保されるものとして転送を許可するようにしている。

【００１５】請求項３記載の発明では（イ）ファイルに付属して記されたそのファイルの機密性に関するファイル側セキュリティレベル情報を解読するファイル側セキュリティレベル情報解読手段と、（ロ）ファイルに付属して記されたそのファイルの出力先に関する出力先情報を解読する出力先情報解読手段と、（ハ）ファイルの出力先ごとにそれらの機密性に関するセキュリティレベル情報を予め格納した出力先セキュリティレベル情報格納手段と、（ニ）送信するファイルのファイル側セキュリ

5

ティレベル情報とその出力先の出力先セキュリティ情報レベルとを照合し両者のレベルが等しいときのみその出力先にファイルの転送を許可するセキュリティ判別手段と、（ホ）セキュリティ判別手段によって転送が許可された出力先にのみファイルを転送するファイル転送手段とをファイル転送装置に具備させる。

【００１６】すなわち請求項３記載の発明では、ファイルに付属して記されたそのファイルのセキュリティレベル情報を得ると共に、ファイルの出力先ごとにそれらの出力先セキュリティレベル情報を得て、ファイルの転送の際には転送先ごとにこれらのレベルを比較し、ファイルのセキュリティレベルが転送先と等しい場合にのみセキュリティが確保されるものとして転送を許可するようにしている。すなわち、セキュリティのレベルが必ずしも上下関係を有さないような場合にも、レベルの等しい転送先にのみファイルを転送することにしてセキュリティの確保を実現している。

【００１７】請求項４記載の発明では、（イ）ファイルに付属して記されたそのファイルの機密性に関するファイル側セキュリティ情報を解読するファイル側セキュリティ情報解読手段と、（ロ）ファイルに付属して記されたそのファイルの出力先に関する出力先情報を解読する出力先情報解読手段と、（ハ）ファイルの出力先ごとにそれらの機密性に関する出力先セキュリティ情報を予め格納した出力先セキュリティ情報格納手段と、（ニ）送信するファイルごとにそれらの出力先とファイル側セキュリティ情報とを対応付けて格納したセキュリティ管理テーブルを作成するセキュリティ管理テーブル作成手段と、（ホ）ファイルの転送要求が生じるたびにセキュリティ管理テーブル作成手段によって作成されたセキュリティ管理テーブルと出力先セキュリティ情報格納手段に格納された出力先セキュリティ情報を照合してファイルごとにセキュリティが確保されるとされた出力先にのみ同報転送を行うファイル同報転送手段とをファイル転送装置に具備させる。

【００１８】すなわち請求項４記載の発明は、複数の転送先に同報転送を行う際のセキュリティの確保を行うためのもので、ファイル側セキュリティ情報を記しておいたファイルからこの情報を得ると共に同報通信を行う転送先の情報を得て、それぞれの転送先のセキュリティ情報との関係を表わした同報通信用のセキュリティ管理テーブルを作成し、同報通信を行う際にこのテーブルを基にして個々の転送先とファイルのセキュリティ情報を照合し、セキュリティが確保されるとされた出力先に対して同報転送を行うようにして機密性の確保を実現している。同報転送は、逐次転送するタイプのものであっても、転送先に一括して転送するものであってもよい。

【００１９】

【実施例】以下実施例につき本発明を詳細に説明する。

【００２０】図１は本発明の一実施例におけるファイル

6

転送装置を使用する通信システムの概要を表わしたものである。本実施例のファイル転送装置１１は通信ケーブル１２に接続されている。この通信ケーブル１２には、第１～第Ｎのワークステーション（ＷＳ）13_1～13_Nの他に第１～第Ｍのプリンタ14_1～14_Mも接続されている。第１～第Ｎのワークステーション13_1～13_Nは、作成したファイルのプリントアウトを希望するときには、そのファイルをファイル転送装置１１に転送する。ファイル転送装置１１は、これを第１～第Ｍのプリンタ14_1～14_Mのうちの指定されたものに転送し、プリントを行わせるようになっている。なお、ファイル転送装置１１はこの図に示した通信ネットワークの範囲内でファイルの転送を行う必要はなく、例えば図示しない通信サーバを介して他の通信システムのプリンタにファイルを転送することも可能である。

【００２１】図２は、ファイル転送装置の構成を原理的に表わしたものである。ファイル転送装置１１は図１に示した第１～第Ｎのワークステーション13_1～13_Nのいずれかからファイル２１が送られてくると、ファイル読み込み部２２がこれを受信するようになっている。ファイル読み込み部２２は、それぞれのファイルからファイル属性レコードとセキュリティ属性レコードを読み込む。そして、ファイル属性レコードからはファイル名等の基本情報２３を得ると共に、セキュリティ属性レコードからはセキュリティ情報２４を入手する。これら基本情報２３およびセキュリティ情報２４は、この段階でセキュリティ管理部２６に送出され、それぞれ基準値として記憶される。

【００２２】ファイル読み込み部２２は、セキュリティ属性レコードに続く実データ２７を受信したファイルから取り出すと、これを転送ファイル記憶部２８に送信する。転送ファイル記憶部２８は、実データ２７を受け取ると、これを内部に配置されたメモリに順次格納し、格納が終了した時点でセキュリティ管理部２６に格納完了通知２９を通知する。

【００２３】セキュリティ管理部２６は、格納完了通知２９を受けると、セキュリティ管理テーブル３１の内容を参照し、送信するファイルのテーブル・エントリを探し出す。そして、該当するテーブル・エントリから順に転送先情報を取り出す。そしてこれらを順に転送部４１に送り、セキュリティ管理テーブル３１で指示されたプリンタ１４に送信する。このときセキュリティ管理部２６は、セキュリティ上問題のないプリンタ１４に対して送信を許可することになる。ファイルの転送制御の詳細は後に説明する。

【００２４】なお、このような構成のファイル転送装置１１全体は図示しないがＣＰＵ（中央処理装置）を備えており、各種制御プログラムを格納したＲＯＭ（リード・オンリ・メモリ）や、各種データやファイルあるいはテーブルを一時的に格納する作業用メモリ等を用いてフ

ァイルの転送制御等の各種制御を行うようになっている。

【００２５】図３は、セキュリティ管理テーブルの構成を表わしたものである。セキュリティ管理テーブル３１には転送するファイルの名称とこれらのファイルの転送先のアドレスＡおよびそれらのセキュリティレベルＬが記されている。セキュリティレベルＬは、図１に示した第１～第Ｍのプリンタ１４$_1$ ～１４$_M$ について、これらの置かれている環境に応じて５段階のうちのいずれかの段階が定められている。これらの段階および知ることができる者の対応は、例えば次のようになる。

【００２６】

【表１】

セキュリティレベル	内容
“Ｌ$_0$”	機密上の問題なし
“Ｌ$_1$”	グループリーダ相当以上
“Ｌ$_2$”	課長相当以上
“Ｌ$_3$”	部長相当以上
“Ｌ$_4$”	最高機密

【００２７】図示しないセキュリティレベルテーブルには第１～第Ｍのプリンタ１４$_1$ ～１４$_N$ のそれぞれのセキュリティレベルの状態が設定されており、これらのレベルは第１～第Ｎのワークステーション１３$_1$ ～１３$_N$ のうちのマスタとなるワークステーションが設定し、またその内容を変更することができる。図３からは、第１の転送先としての第１のプリンタ１４$_1$ のセキュリティレベルが“Ｌ$_2$”に設定されていることと、第Ｎのプリンタ１４$_N$ のセキュリティレベルが“Ｌ$_0$”に設定されていることがわかる。例えば第１のプリンタ１４$_1$ は、同一の部で複数または単一の課長が人事関係の書類等を受信するために使用することを前提としたものであり、課長職以外の者が使用することを前提としていないためにセキュリティレベルが若干高くなっている。これに対して第Ｎのプリンタ１４$_N$ は、通常の研究者等が自由に使用することができる場所に配置されているので、セキュリティレベルが最低となっている。

【００２８】もちろん、セキュリティレベルの区分は表１に示した以外で各種可能であり、例えば“Ｌ$_0$”を一般レベル、“Ｌ$_1$”を取扱注意レベル、“Ｌ$_2$”を社外秘レベル、“Ｌ$_3$”をマル秘レベル、“Ｌ$_4$”を極秘レベルとすることも可能である。レベルの数もこれに限るものではない。

【００２９】図４は、ファイル転送装置が受信するファイルの構成を表わしたものである。ファイル転送装置１１に送られるファイル３２はファイルの内容をなす実データ３３にファイル属性レコード３４とセキュリティ属性レコード３５が付加された構成となっている。ファイル属性レコード３４には、ファイル名やファイルの所有者および希望する送信先等の情報が記されており、セキュリティ属性レコード３５にはそのファイルの５段階のセキュリティレベルＬ$_0$ ～Ｌ$_4$ のいずれかが記されている。ただし、本実施例のシステムでは、セキュリティレベルＬの記載がない場合には、これをセキュリティレベルＬ$_0$ と擬制することにしている。すなわち、本実施例のファイル転送装置は図４に示したファイル構成を有していない既存のファイルもセキュリティレベルをＬ$_0$ と義制することでそれらの活用を図っている。

【００３０】図５は、ファイル転送装置によるファイルの転送制御の様子を具体的に表わしたものである。前記したように一連のファイルに対する格納完了通知があったら（ステップＳ１０１；Ｙ）、２つの変数ａ、ｂの値がそれぞれ“１”に初期化される（ステップＳ１０２）。これらの変数ａ、ｂは前記した作業用メモリの所定の領域に格納されている。前記したＣＰＵは図３に示したセキュリティ管理テーブル３１の第１のテーブルエントリのファイルＦ$_1$ についてのセキュリティレベルＬ$_f$ を読み出す（ステップＳ１０３）。これは、図４に示したそのファイル３２のセキュリティ属性レコード３５に格納されている。そして、第１番目の転送先（第１のプリンタ１４$_1$ ）のセキュリティレベルＬ$_P$ を読み出す（ステップＳ１０４）。ここではセキュリティレベルＬ$_P$ は、“Ｌ$_0$”である。そして、セキュリティレベルＬ$_f$ がセキュリティレベルＬ$_P$ と等しいか、これよりも低い場合には（ステップＳ１０５；Ｎ）、セキュリティ上の問題が発生しないので、そのファイルＦ$_1$ を該当する転送先に転送する（ステップＳ１０６）。

【００３１】この例の場合、第１のテーブルエントリのファイルＦ$_1$ についてのセキュリティレベルＬ$_f$ が“Ｌ$_1$”であるとする。すると、“Ｌ$_1$”は転送先のセキュリティレベルＬ$_P$ としての“Ｌ$_2$”よりも小さいので、セキュリティ上の問題が発生しない。したがって、ファイルＦ$_1$ は転送部４１から第１番目の転送先（第１のプリンタ１４$_1$ ）に転送されることになる。このとき、セキュリティ管理テーブル３１に登録されたその転送先のアドレスＡ$_1$ が転送部４１に通知されることはもちろんである。

【００３２】この後、変数ｂの値が“１”だけカウントアップされて、“２”となる（ステップＳ１０７）。ＣＰＵはファイルＦ$_1$ について２番目の転送先があるかどうかをセキュリティ管理テーブル３１で調べる（ステップＳ１０８）。そして、転送先が存在する限り、ステップＳ１０４に戻って同様のチェックが行われ、ステップＳ１０５の条件を満たす場合にはその転送先にファイルＦ$_1$ の転送が行われることになる。

【００３３】他の例としてファイルＦ$_1$ を第Ｎのプリンタ１４$_N$ に転送する指示に対する制御内容を説明する。この場合にはファイルＦ$_1$ についてのセキュリティレベルＬ$_f$ が“Ｌ$_1$”であるのに対して、第ｎ番目の転送先（第Ｎのプリンタ１４$_N$ ）のセキュリティレベルＬ$_P$ は

“L_0”である。ステップＳ１０５の判断ではファイルF_1についてのセキュリティレベルL_fの方が大きくなり、転送先はセキュリティ上問題があることになる（Ｎ）。したがって、この場合には転送部４１による第Ｎのプリンタ１４$_N$へのファイルF_1の転送が許可されず、ステップＳ１０７に直ちに進んで次の転送先についての処理が行われることになる。

【００３４】この例の場合には、ファイルF_1について第ｎ番目の転送先（第Ｎのプリンタ１４$_N$）が最終の転送先になるので（ステップＳ１０８；Ｎ）、今度は変数ａが“１”だけカウントアップされて“２”となる（ステップＳ１０９）。セキュリティ管理テーブル３１には次に転送すべきファイルに関するデータがセットされているので（ステップＳ１１０；Ｙ）、ステップＳ１０３に進んで第２のエントリテーブルのファイルF_2についての同様の転送制御が行われることになる（ステップＳ１０３～Ｓ１１０）。このようにしてセキュリティ管理テーブル３１にセットされたすべてのファイルについて転送処理が終了すると（ステップＳ１１０；Ｎ）、一連のファイル転送についての制御が終了する（エンド）。

【００３５】なお、以上説明した実施例では図５のステップＳ１０５でセキュリティレベルの判別を行うとき、ファイルの転送先のレベルがファイルの転送に際して要求されるレベル以上であればそのファイルの転送を行うことにした。これは、例えばある課長に配付するファイルを部長が所有するプリンタに出力してもセキュリティ上問題を生じないという前提にたったものである。しかしながら、構築するシステムの内容によってはセキュリティレベルが必ずしもレベルの上下関係で定義付けることができず、同一セキュリティレベルのプリンタあるいは転送先にのみ出力されることが妥当な場合も存在する。このようなシステムでは本発明のファイル転送装置は同一のセキュリティレベルの転送先のみに転送するような制御を行ってもよい（請求項３記載の発明）。

【００３６】また、実施例ではファイルの転送先がプリンタである場合を説明したが、これに限るものではなく、ディスプレイ装置や、場合によっては受信したファイルの編集を行うワードプロセッサ等の文書作成装置を転送先とすることも可能であり、これらについても本発明を適用することができる。例えば図１に示したシステムでは、例えば第１のワークステーション１３$_1$が作成したファイルが第４～第８のワークステーション１３$_4$～１３$_8$に同報通信されるような場合にもセキュリティ上問題があれば本発明を有効に活用することができる。

【００３７】更に実施例ではファイルの転送先がセキュリティ上適格であってもビジィ等によって転送が失敗した場合を説明しなかった。このような場合には転送の失敗した転送先と該当するファイル名をセキュリティ管理テーブル３１に残しておけば、次の格納完了通知（ステップＳ１０１）が発生したとき等のついでのときに、これらのファイルを未送信の転送先に転送することができる。セキュリティ上問題とされないすべての転送先にファイルの転送を行ったら、セキュリティ管理テーブル３１における該当するエントリを削除してよいこともちろんである。また、セキュリティ上問題があるとしてファイルの転送を行わなかった転送先に対しては、その旨の通知を別途行ってもよいことは当然である。

【００３８】また実施例では転送先に順次ファイルを転送していく逐次同報通信タイプの同報転送について説明したが、個々の転送先についてセキュリティをチェックし、合格したものについて一斉にそのファイルを転送する一括同報通信タイプの同報転送に本発明を適用することができることは当然である。ローカルエリアネットワークでこのような一括同報通信を行うためには、例えばそれぞれのプリンタ等の受信先の装置に共通したアドレスを付けてファイルの転送を行うか、これらのアドレスを併記してファイルの転送を行い、これら該当する装置がそのファイルを共通して取り込むようにすればよい。

【００３９】

【発明の効果】以上説明したように請求項１記載の発明によれば、ファイル側セキュリティ情報を記しておいたファイルからこの情報を得ると共に、ファイルの出力先ごとにそれらの出力先セキュリティ情報を得て、ファイルの転送の際にはこれらを比較しセキュリティが確保されるとされた出力先にのみファイルを転送することにしたので、ファイルの送信者が転送先のセキュリティに関する知識を持たなくても機密性の保持を確保することができる。

【００４０】また、請求項２記載の発明によれば、ファイルに付属して記されたそのファイルのセキュリティレベル情報を得ると共に、ファイルの出力先ごとにそれらの出力先セキュリティレベル情報を得て、ファイルの転送の際には転送先ごとにこれらのレベルを比較し、ファイルのセキュリティレベルが転送先と等しいか転送先の方が高い場合にはセキュリティが確保されるものとして転送を許可するようにした。このようにセキュリティの強さについてレベルを設定したので、ファイルの送信者が転送先のセキュリティに関する知識を持たなくても、その設定したレベル以上のセキュリティを確保することのできる転送先のみに転送が行われることになり、機密性の保持を確保することができる。

【００４１】更に請求項３記載の発明によれば、ファイルに付属して記されたそのファイルのセキュリティレベル情報を得ると共に、ファイルの出力先ごとにそれらの出力先セキュリティレベル情報を得て、ファイルの転送の際には転送先ごとにこれらのレベルを比較し、ファイルのセキュリティレベルが転送先と等しい場合にのみセキュリティが確保されるものとして転送を許可するようにした。このようにセキュリティの強さについてレベルを設定したので、ファイルの送信者が転送先のセキュリ

ティにレベルを設け、その設定したレベルが一致する転送先のみに転送を行うことにしたので、必ずしもセキュリティのレベルが上下関係を有さないような場合でも機密性の保持を確保することができる。

【００４２】また請求項４記載の発明によれば、ファイル側セキュリティ情報を記しておいたファイルからこの情報を得ると共に同報通信を行う転送先の情報を得て、それぞれの転送先のセキュリティ情報との関係を表わした同報通信用のセキュリティ管理テーブルを作成し、同報通信を行う際にこのテーブルを基にして個々の転送先とファイルのセキュリティ情報を照合し、セキュリティが確保されるとされた出力先に対して同報転送を行うようにした。したがって、セキュリティ管理テーブルを用いて同報通信を円滑に行うことができる。また、テーブルに送信の成功の有無を記録するようにすれば、未送信の転送先についてもセキュリティを確保しながら後の時点で転送を行うことができる。

【００４３】更に、同報通信の場合には複数の転送先にファイルの転送を行うので、これら転送先のセキュリティに関する情報を得にくいが、請求項４記載の発明ではファイル転送装置側にこれに関するデータが用意されており、これを基にしてセキュリティ管理テーブルが作成＊

＊されるので、送信者はファイルにセキュリティ情報を記しておくことと、希望する転送先を指定するだけでよく、同報通信作業が効率化するという効果もある。

【図面の簡単な説明】

【図１】　本発明の一実施例におけるファイル転送装置を使用する通信システムの概要を表わしたシステム構成図である。

【図２】　本実施例のファイル転送装置の構成を原理的に表わしたブロック図である。

【図３】　本実施例におけるセキュリティ管理テーブルの構成を表わした説明図である。

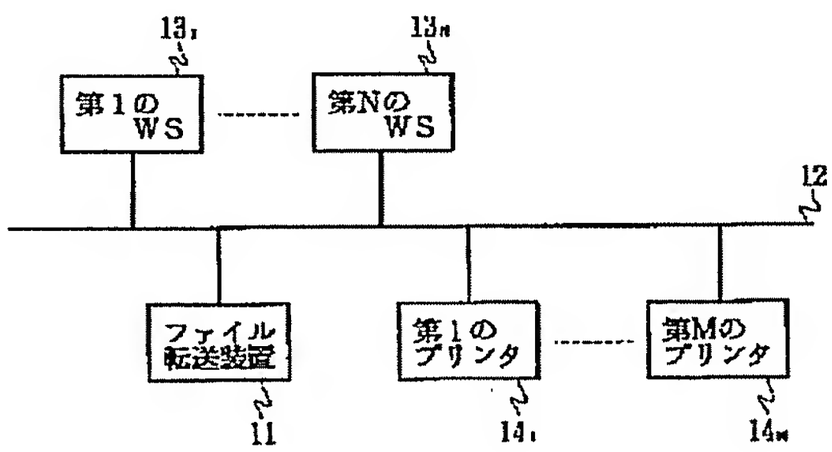
【図４】　本実施例のファイル転送装置が受信するファイルの構成を表わした説明図である。

【図５】　ファイル転送装置によるファイルの転送制御の様子を具体的に表わした流れ図である。

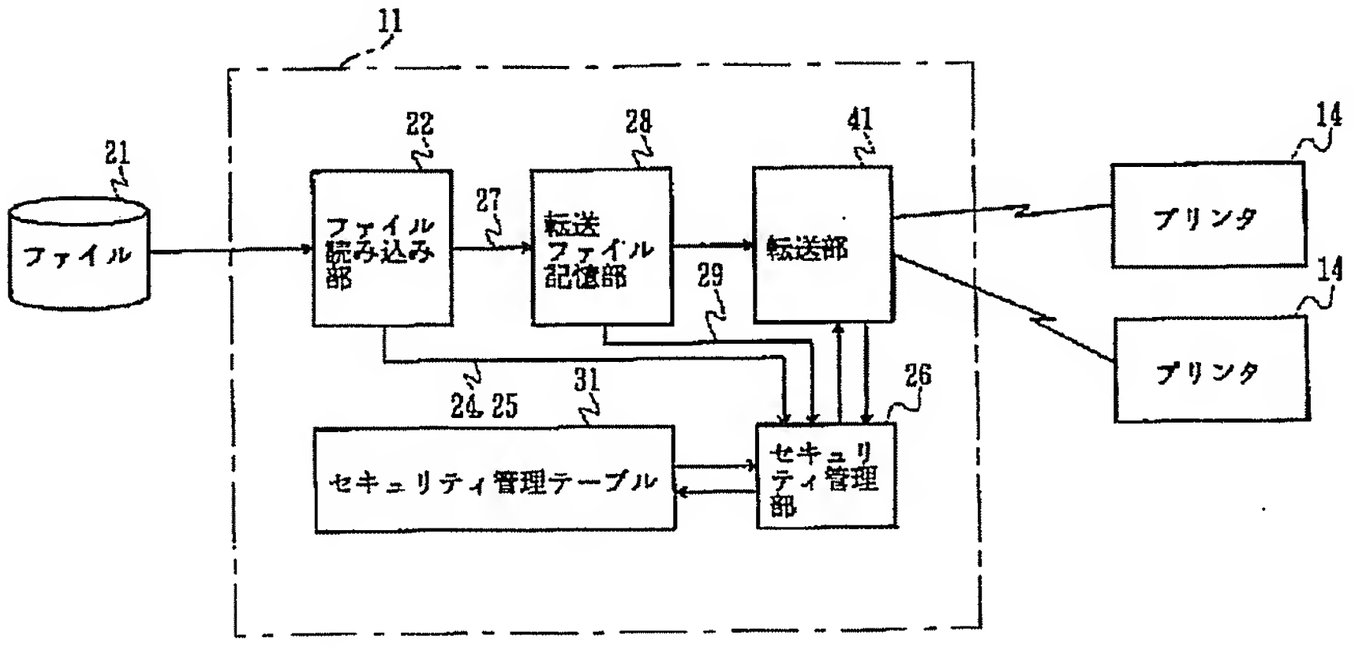
【符号の説明】

１１…ファイル転送装置、１４$_1$ ～１４$_M$ …第１～第Ｍのプリンタ、２１、３２…ファイル、２２…ファイル読み込み部、２６…セキュリティ管理部、２８…転送ファイル記憶部、３１…セキュリティ管理テーブル、３５…セキュリティ属性レコード、Ｌ…セキュリティレベル

【図１】



【図２】

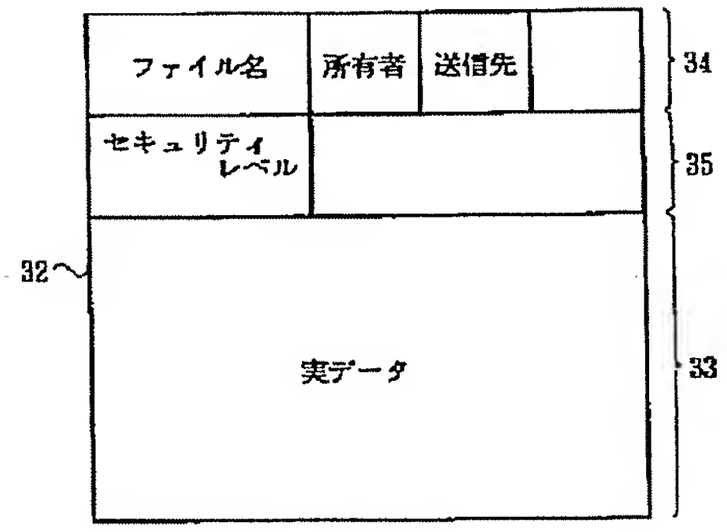


【図３】

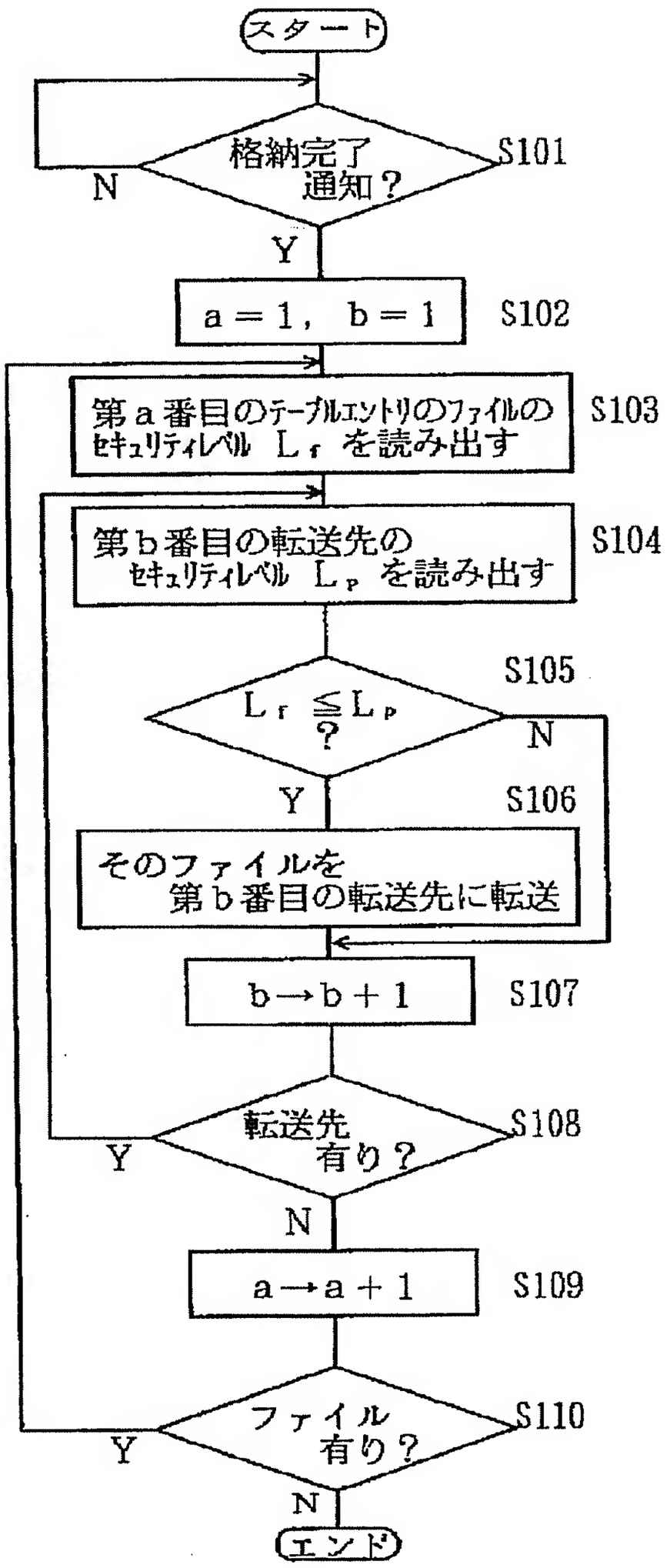
31

ファイル名	第１の転送先		.....	第ｎの転送先	
	アドレス	セキュリティレベル		アドレス	セキュリティレベル
F_1	A_2	L_2	.....	A_N	L_0
F_2	A_N	L_0			
.....					

【図４】



【図５】


スタート
格納完了通知？
S101
N
Y
a＝1，　b＝1
S102
第ａ番目のテーブルエントリのファイルのセキュリティレベル　Ｌｒ　を読み出す
S103
第ｂ番目の転送先のセキュリティレベル　Ｌｐ　を読み出す
S104
Ｌｒ ≦ Ｌｐ ？
S105
N
Y
S106
そのファイルを第ｂ番目の転送先に転送
b→b＋1
S107
転送先有り？
S108
Y
N
a→a＋1
S109
ファイル有り？
S110
Y
N
エンド